Ciberseguridad educativa a través del blindaje y detección de intrusos de redes informáticas

Educational cybersecurity through the protection and intrusion detection of computer networks

Victor Azareel Ramirez Anaya
Universidad Autónoma del Estado de México
ORCID: 0009-0005-3720-0713
victorazareelr@gmail.com
Laura Cecilia Méndez Guevara
Universidad Autónoma del Estado de México
ORCID: 0000-0002-4190-7157
lcmendezg@uaemex.mx

RESUMEN

La ciberseguridad educativa se ha convertido en una prioridad ante el incremento de amenazas en redes escolares. En algunas instituciones de nivel medio superior, se ha detectado que, la falta de control en el acceso, la presencia de puertos abiertos y el uso inadecuado de contraseñas generan vulnerabilidades que comprometen la integridad, la disponibilidad y confidencialidad de la información. Este estudio propone fortalecer la seguridad mediante el blindaje de redes informáticas y la implementación de sistemas de detección de intrusos (IDS), como Suricata. A través de un enfoque metodológico descriptivo y experimental se realiza un diagnóstico de la infraestructura de red, seguido de la configuración e implementación del IDS para monitorear el tráfico en tiempo real y detectar actividades maliciosas. Los resultados esperados incluyen la reducción de incidentes de seguridad, la optimización del rendimiento de la red y una mayor capacidad de respuesta ante amenazas. El blindaje de redes, combinado con la detección de intrusos, permite prevenir ataques y también fortalecer la gestión tecnológica en entornos educativos. En conclusión, la adopción de estas estrategias contribuye a crear espacios digitales más seguros, confiables y eficientes, favoreciendo el desarrollo académico y la protección de los datos institucionales.

Palabras clave: Ciberseguridad Educativa, Blindaje de Redes, Detección de Intrusos.

ABSTRACT

Educational cybersecurity has become a priority due to the increasing number of threats in school networks. In upper secondary education institutions, the lack of access control, the presence of open ports, and the improper use of passwords create vulnerabilities that compromise the integrity,

availability, and confidentiality of information. This study proposes strengthening security through network hardening and the implementation of intrusion detection systems (IDS), such as Suricata. Through a mixed methodological approach exploratory, descriptive, and experimental a diagnosis of the network infrastructure is carried out, followed by the configuration and implementation of the IDS to monitor traffic in real time and detect malicious activities. Expected results include a reduction in security incidents, optimization of network performance, and an improved capacity to respond to threats. Network hardening, combined with intrusion detection, not only helps prevent attacks but also strengthens technological management in educational environments. In conclusion, the adoption of these strategies contributes to creating safer, more reliable, and efficient digital spaces, promoting academic development and the protection of institutional data.

Keywords: Educational Cybersecurity, Network Hardening, Intrusion Detection.

INTRODUCCIÓN

Dentro del contexto de las escuelas de nivel medio superior, el constante acceso a las herramientas digitales por parte de los estudiantes ha evidenciado diversas vulnerabilidades en la seguridad de las redes institucionales. A partir de la observación realizada sobre el uso de laboratorios de cómputo de un plantel educativo, fue posible observar de cerca las fallas que comprometen tanto el rendimiento como la protección de la infraestructura tecnológica.

Una de las principales debilidades detectadas es la falta de control sobre la conexión de equipos personales a la red escolar. Esta práctica, se realiza sin ningún tipo de autorización o filtro, provocando una sobrecarga en el sistema, reduce la velocidad de navegación y afecta la experiencia de toda la comunidad educativa. Además, facilita el ingreso de dispositivos que podrían estar infectados o mal configurados, lo que incrementa los errores cometidos por los propios usuarios.

A lo anterior, se añaden dos fallas estructurales relevantes; por un lado, la presencia de puertos de red abiertos sin la regulación necesaria, lo que representa una puerta de entrada para accesos no autorizados y posibles ciberataques, cuyas consecuencias van desde la pérdida de información confidencial hasta interrupciones prolongadas del servicio. En otro sentido, el manejo deficiente de las claves de acceso, las cuales circulan libremente entre el alumnado, imposibilitando rastrear quién realiza determinadas acciones dentro de la red y debilitando gravemente los mecanismos de seguridad.

Lo anterior, denota la urgencia de implementar políticas más estrictas y medidas técnicas adecuadas dentro de las instituciones de educación media superior, donde la cantidad de estudiantes es elevada y la red se ha convertido en una herramienta indispensable para el aprendizaje. Frente a este panorama, la presente investigación ofrece soluciones concretas, diseñadas específicamente para

cada una de las fallas señaladas, para garantizar una red más segura, eficiente y confiable en este nivel educativo.

En la actualidad, la seguridad de la información se ha convertido en un aspecto crítico para las instituciones educativas en especial aquellas de nivel medio superior, debido al incremento de las denominadas ciberamenazas que son ataques dirigidos en este caso a las redes académicas. Según Symantec (2022), el sector educativo es uno de los más vulnerables, ya que el 60% de las instituciones reportaron al menos un incidente de seguridad en el último año. Ante esta problemática, emergen los sistemas de detección de intrusiones (IDS, por sus siglas en inglés) como una solución esencial para proteger la infraestructura tecnológica y garantizar la confidencialidad, integridad y disponibilidad de los datos.

Suricata, es un software IDS de código abierto y alto rendimiento, se ha posicionado como una herramienta eficaz para la monitorización de redes y la detección de actividades maliciosas. Su capacidad para analizar tráfico en tiempo real, junto con su flexibilidad para adaptarse a diferentes entornos, lo convierte en una opción viable para instituciones educativas como la que ha sido objeto de este análisis. Este tipo de centros, al igual que muchas otras escuelas de nivel medio superior, maneja una gran cantidad de datos sensibles desde información personal de estudiantes y docentes hasta registros administrativos, lo que los convierte en un objetivo potencial para ciberataques, especialmente cuando presentan las fallas de seguridad previamente descritas.

El marco teórico de esta investigación se sustenta en tres pilares fundamentales:

1. la teoría de la seguridad informática, que aborda los principios y prácticas para proteger sistemas y redes;
2. los sistemas de detección de intrusiones, con un enfoque en Suricata y su arquitectura basada en reglas y firmas; y
3. la aplicación de estas tecnologías en entornos educativos, considerando las particularidades de las redes académicas y los desafíos que enfrentan.

Autores como Stallings (2021) destacan que "la implementación de un IDS no solo debe enfocarse en la detección de amenazas, sino también en la capacidad de respuesta y la prevención proactiva" (p. 78).

Esta investigación busca contribuir al campo de la ciberseguridad en el ámbito de la educación media superior, proporcionando un modelo de implementación de Suricata adaptado a las necesidades de instituciones que presentan problemáticas similares a las aquí diagnosticadas. A través de este marco teórico, se espera sentar las bases para comprender la importancia de los IDS en la protección de redes académicas y justificar la elección de Suricata como herramienta central en este proyecto.

La seguridad de redes informáticas se refiere a la protección de la infraestructura y los datos que circulan en una red frente a accesos no autorizados, ataques maliciosos y fallos técnicos. Según

KeepCoding Bootcamps (2023), garantizar la integridad, disponibilidad y confidencialidad de los datos es esencial en cualquier entorno que dependa de sistemas de información.

1.1 Principales Amenazas a la Seguridad de Redes

Las redes están expuestas a diversas amenazas, tales como:

- Accesos no autorizados: Conexión de dispositivos sin autorización que comprometen la seguridad del sistema.
- Puertos abiertos: Facilitan el acceso a atacantes externos.
- Contraseñas débiles o compartidas: Reducen la capacidad de controlar y restringir accesos.

Estas vulnerabilidades generan riesgos de pérdida de datos, interrupciones en el servicio y ataques cibernéticos, lo que subraya la importancia de implementar soluciones robustas de seguridad (CEC, 2023).

Un Sistema de Detección de Intrusos (IDS) es una herramienta diseñada para monitorear y analizar el tráfico de red con el fin de identificar actividades sospechosas o maliciosas. Los IDS se clasifican en:

- IDS basado en red (NIDS): Monitorean el tráfico de red en tiempo real.
- IDS basado en *host* (HIDS): Supervisan actividades en sistemas específicos.

Los IDS son esenciales para detectar y prevenir ataques antes de que causen daños significativos, siendo una de las soluciones más efectivas en seguridad informática (Blog elhacker.NET, 2021).

Entre los IDS más utilizados se encuentran Snort, Suricata y Zeek. Suricata se destaca por su flexibilidad, capacidad de Inspección Profunda de Paquetes (Deep Packet Inspection) que es una técnica avanzada que analiza no solo las cabeceras de los paquetes de red (como direcciones IP o puertos), sino también el contenido completo como son datos, protocolos, aplicaciones ocultas y su integración con otras herramientas de seguridad. Además, es compatible con las reglas de Snort, lo que facilita la migración y personalización (CEC, 2023).

Suricata es un IDS/IPS de código abierto desarrollado por la *Open Information Security Foundation* (OISF). Entre sus características principales destacan:

- Inspección profunda de paquetes (DPI): Permite analizar el contenido de los paquetes en busca de patrones sospechosos.
- Compatibilidad con Sistemas de Gestión de Eventos e Información de Seguridad (SIEMs) las cuales son plataformas que recolectan y analizan datos de seguridad de múltiples fuentes como firewalls, servidores, IDS/IPS para monitorear, detectar y dar respuestas rápidas a las posibles amenazas además de facilitar la integración con sistemas existentes, optimizando el monitoreo y análisis.
- Rendimiento escalable: Puede manejar grandes volúmenes de tráfico, siendo ideal para redes de alta velocidad.

- Comunidad activa: Asegura actualizaciones frecuentes y soporte técnico continuo (KeepCoding Bootcamps, 2023).

Suricata ofrece varias ventajas en comparación con otras soluciones:

- Flexibilidad y personalización: Su arquitectura modular permite ajustar configuraciones según necesidades específicas.
- Código abierto: Permite adaptaciones sin costos adicionales.
- Eficiencia operativa: Mejora la capacidad de detección de amenazas y reduce incidentes de seguridad (Guías Open Source, 2023).

Autores expertos indican que la investigación científica debe ser sistemática, rigurosa y basada en evidencia. Este enfoque permite analizar las redes informáticas como sistemas complejos que interactúan con su entorno y requieren soluciones integrales.

La teoría de los sistemas vivos propone que los sistemas deben ser adaptativos y capaces de evolucionar frente a nuevas amenazas. En el contexto de redes, un IDS como Suricata se ajusta a este enfoque, ya que permite actualizaciones constantes para enfrentar amenazas emergentes. (García, 2020).

Suricata se utiliza ampliamente en:

- Entornos educativos: Para enseñar y estudiar seguridad informática.
- Empresas: Como una herramienta clave en centros de operaciones de seguridad (SOC).
- Investigación y desarrollo: Para probar nuevas estrategias de detección y prevención de intrusos (Blog elhacker.NET, 2021).

Para las preparatorias y bachilleratos, la seguridad de la red informática es una prioridad crítica. Durante el tiempo de estudio y prácticas en los laboratorios de informática, se han identificado varias vulnerabilidades.

Para reafirmar lo anterior, se desarrollan los criterios de Ackoff y Miller, mismos que profundizan en la reflexión de la implementación de un IDS. Ackoff, conocido por su trabajo en teoría de sistemas y cibernética, enfatiza la importancia de un enfoque holístico en la gestión de sistemas complejos. Según sus criterios, la implementación de un IDS debe considerar no solo los aspectos técnicos, sino también los organizacionales y humanos. Esto incluye la capacitación del personal, la integración con otros sistemas de seguridad y la evaluación continua de su efectividad.

Por otro lado, Miller, con su teoría de los sistemas vivos, sugiere que cualquier sistema de seguridad debe ser adaptable y capaz de evolucionar frente a nuevas amenazas. En este contexto, un IDS como Suricata, con su capacidad de actualización y personalización, cumple con estos criterios al ofrecer una solución flexible y escalable que puede ajustarse a las necesidades cambiantes de las preparatorias y bachilleratos, así como de la institución educativa en general.

La implementación de un Sistema de Detección de Intrusos (IDS) es conveniente debido a las siguientes razones:

- Dependencia tecnológica: En las últimas décadas, la informática ha ganado terreno en todas las áreas del quehacer humano, incluyendo la educación. La seguridad de la red es esencial para garantizar el buen funcionamiento de las actividades académicas y administrativas en las preparatorias y bachilleratos.
- Vulnerabilidades identificadas: La falta de control sobre los accesos a la red, los puertos abiertos sin restricciones adecuadas y las contraseñas conocidas y compartidas entre los estudiantes son problemas que requieren una solución urgente para evitar el uso indebido de los recursos y posibles ataques cibernéticos.

METODOLOGÍA

La investigación se fundamentará en el enfoque filosófico de Bunge, quien propone una visión sistémica y científica de la investigación. Según Bunge, la investigación debe ser un proceso sistemático, riguroso y basado en la evidencia. Este enfoque se complementará con la perspectiva pragmática, que busca soluciones prácticas y aplicables a problemas reales.

Desde un enfoque filosófico, este artículo adopta una perspectiva sistémica y pragmática. La perspectiva sistémica, inspirada en la teoría de sistemas vivos de Miller, considera la red de datos como un sistema complejo y dinámico que debe ser protegido de manera integral. Este enfoque permite entender cómo interactúan los diferentes componentes de la red y cómo se pueden adaptar para enfrentar nuevas amenazas.

Por otro lado, el enfoque pragmático se centra en la aplicabilidad y efectividad de las soluciones propuestas. En lugar de limitarse a un análisis teórico, este artículo busca implementar y probar soluciones prácticas que mejoren la seguridad de la red de datos en las preparatorias y bachilleratos. La elección de Suricata como IDS se justifica no solo por sus capacidades técnicas, sino también por su flexibilidad y adaptabilidad a las necesidades específicas de estos planteles (Cruzito, 2020).

El tipo de investigación será del tipo exploratoria debido a que inicialmente, se realizará una investigación exploratoria para comprender el estado actual de la seguridad de la red de datos en las preparatorias y bachilleratos. Esta fase permitirá identificar las principales vulnerabilidades y amenazas (Stebbins, 2001).

Además, es descriptiva ya que, se describirán detalladamente las características de la red y las amenazas identificadas. Esta descripción incluirá la topología de la red, los componentes críticos y los patrones de tráfico (Babbie, 2020).

Complementariamente, del tipo explicativa, donde se buscará explicar las causas de las vulnerabilidades y amenazas, así como la necesidad de implementar un Sistema de Detección de Intrusos (IDS) (Yin, 2018).

Y por último experimental envase a la implementación y prueba del IDS Suricata en la red de datos, evaluando su efectividad y rendimiento (Shadish, Cook, & Campbell, 2002).

Mientras que los métodos son del tipo documental porque se realizará una revisión exhaustiva de la literatura existente sobre seguridad de redes, IDS y específicamente sobre Suricata. Esto incluirá artículos académicos, libros, documentación técnica y estudios de caso (Parra, 2020).

También inductivo ya que, a partir de la observación y análisis de datos recolectados durante el diagnóstico de la red, se generarán hipótesis sobre las vulnerabilidades y amenazas presentes (Parra, 2020).

Y deductivo ya que se aplicarán teorías y modelos existentes sobre seguridad de redes y detección de intrusos para diseñar y justificar la implementación del IDS Suricata en las preparatorias y bachilleratos (Parra, 2020).

Un Sistema de Detección de Intrusiones (IDS, por sus siglas en inglés), un componente esencial en la defensa contra amenazas cibernéticas. En concreto un IDS es un sistema diseñado para monitorear el tráfico de red o las actividades en un sistema informático con el objetivo de detectar comportamientos maliciosos o anomalías que puedan indicar un intento de intrusión.

A diferencia de un firewall, que actúa como una barrera para prevenir el acceso no autorizado, un IDS se enfoca en identificar actividades sospechosas una vez que han ocurrido o están en proceso. Según Stallings (2021), un IDS no solo detecta intrusiones, sino que también proporciona alertas para que los administradores puedan tomar medidas correctivas (p. 123). Esto lo convierte en una herramienta reactiva y proactiva al mismo tiempo, ideal para entornos donde los recursos humanos y técnicos pueden ser limitados, como en las preparatorias y bachilleratos.

Figura 1

Panorama de sistemas de detección de intrusiones (IDS)

Nota: Desarrollo del autor

La importancia de un IDS radica en su capacidad para proporcionar visibilidad sobre lo que ocurre en una red o sistema. En palabras de Smith et al. (2020), un IDS es como una cámara de vigilancia en el mundo digital: no previene el crimen, pero proporciona evidencia crucial para responder a él (p. 56). Además, los IDS son esenciales para cumplir con normativas protege la reputación de las instituciones educativas, ya que un solo incidente de seguridad puede tener consecuencias devastadoras, desde pérdidas financieras hasta daños a la imagen pública. En el caso específico de las preparatorias y bachilleratos, la implementación de un IDS contribuye a salvaguardar la información de estudiantes y docentes, garantizando la continuidad de las actividades académicas.

Figura 2

Componentes principales de un IDS

Nota: Desarrollo del autor

Flujo de trabajo explicado

Sensores (NIDS/HIDS):

NIDS (Red): Como cámaras de seguridad en la calle, revisan el tráfico de la red (por ejemplo, paquetes sospechosos).

HIDS (Dispositivo): Como alarmas en puertas o ventanas, monitorean actividades dentro de un dispositivo (por ejemplo, cambios en archivos importantes).

Motor de análisis:

Recibe datos de los sensores y decide si es una amenaza. Usa dos métodos:

Firmas: Compara con patrones conocidos (como buscar la huella de un ladrón).

Anomalías: Detecta comportamientos raros (por ejemplo, un usuario que se conecta a las 3:00 a.m.).

Base de datos de firmas:

- Una lista actualizada de "huellas" de ataques conocidos (por ejemplo, virus, exploits).
- Consola de administración (el panel de control):
- Muestra alertas al administrador (por ejemplo, "¡Intento de ataque SQL detectado!").
- Permite bloquear direcciones IP, actualizar firmas o ajustar sensores.
- El motor de análisis consulta la base de firmas y confirma que es un ataque.
- La consola recibe la alerta y el administrador actúa
- Analogía para su comprensión
- Imagina que el IDS es como la seguridad de un banco:
- Sensores: Cámaras y guardias (ven lo que pasa).
- Motor de análisis: El sistema que revisa las grabaciones y dice "¡Ese gesto es de un ladrón!".
- Base de firmas: Un manual con fotos de ladrones conocidos.
- Consola: El jefe de seguridad que recibe el aviso y llama a la policía.

En el caso de las preparatorias y bachilleratos, esta analogía resulta especialmente útil: los sensores vigilan constantemente la actividad en la red educativa, el motor de análisis detecta comportamientos anómalos (como un estudiante intentando acceder a áreas restringidas), y la consola permite al personal de informática tomar medidas inmediatas para proteger los recursos institucionales y la información de la comunidad escolar.

Figura 3

Panorama de sistemas de detección de intrusiones

Nota: Desarrollo del autor

En el contexto de las preparatorias y bachilleratos, la combinación de ambos métodos puede resultar especialmente efectiva. La detección basada en firmas permite identificar amenazas conocidas, como intentos de acceso no autorizado o malware común, mientras que la detección por anomalías ayuda a detectar comportamientos inusuales en la red, como un flujo anómalo de datos en horarios no habituales, lo que podría indicar un ataque emergente.

Una dirección IP (Internet Protocol address) es un identificador numérico único asignado a cada dispositivo conectado a una red que utiliza el Protocolo de Internet (IP) para comunicarse. Funciona como una "dirección postal" que permite que los dispositivos (como computadoras, smartphones, routers, servidores, etc.) se encuentren y intercambien datos en una red, ya sea local (LAN) o global (Internet). En escuelas de nivel preparatorias y/o bachilleratos, comprender el concepto de dirección IP es fundamental para gestionar el acceso a la red institucional y rastrear posibles incidentes de seguridad.

Figura 4

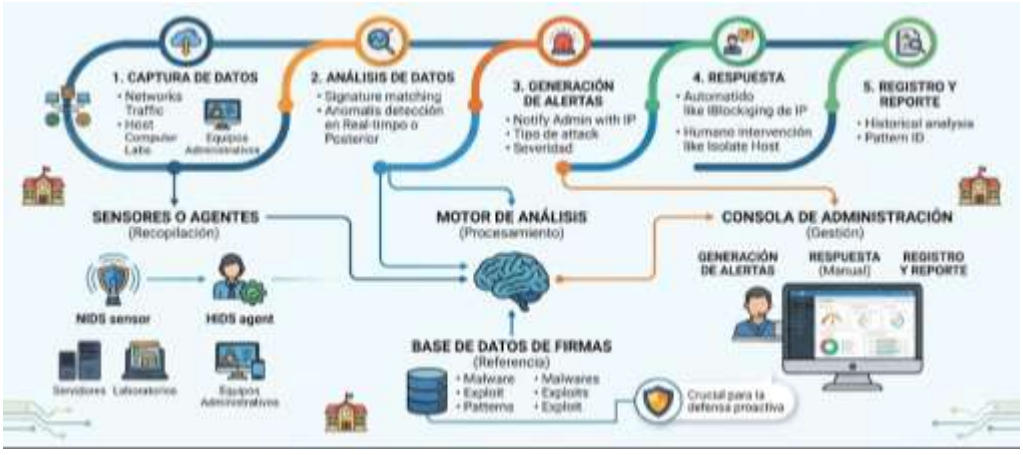
Características clave

Nota: Desarrollo del autor

En las preparatorias y bachilleratos, el conocimiento de las direcciones IP permite a los administradores de red identificar qué dispositivos están conectados en un momento dado, detectar accesos no autorizados y establecer políticas de seguridad más efectivas. Por ejemplo, si un IDS genera una alerta sobre actividad sospechosa proveniente de una IP específica, el equipo de informática puede localizar rápidamente el dispositivo involucrado y tomar medidas correctivas, como bloquear esa dirección o aislar el equipo de la red.

Figura 5

Flujo de trabajo de un IDS



Nota: Desarrollo del autor

La correcta ejecución de este flujo de trabajo permite que las preparatorias y bachilleratos mantengan un entorno digital seguro para estudiantes, docentes y personal administrativo. Al contar con un IDS bien configurado, las instituciones pueden detectar intentos de intrusión de manera temprana,

responder oportunamente y documentar incidentes para fortalecer sus estrategias de seguridad a futuro. Esto no solo protege los recursos tecnológicos, sino que también contribuye a generar confianza en la comunidad educativa respecto al manejo de la información y la continuidad de las operaciones académicas.

Figura 6

Comparativo de IDS en el ámbito académico

Nota: Desarrollo del autor

RESULTADOS Y DISCUSIÓN

Del diagnóstico de la infraestructura de red en el plantel educativo de nivel medio superior, se llegó a la resolución de una falta de control en el acceso de dispositivos personales además que estudiantes conectan equipos personales a la red escolar sin autorización ni filtros, lo que genera sobrecarga, reducción de velocidad de navegación y posible ingreso de dispositivos infectados esto desemboco en el hallazgo de puertos de red abiertos sin regulación, puertos abiertos que representan puertas de entrada para accesos no autorizados, aumentando el riesgo de ciberataques, pérdida de información confidencial e interrupciones del servicio además de esto el manejo deficiente de contraseñas claves de acceso que circulan libremente entre el alumnado, lo que impide rastrear acciones individuales dentro de la red y debilita gravemente los mecanismos de seguridad esto provoca una alta vulnerabilidad del sector educativo y confirmó que con base en literatura (Symantec, 2022), que el 60% de las instituciones educativas han reportado al menos un incidente de seguridad en el último año, validando la urgencia de intervenir, esto evidencio que la red institucional carece de sistemas de detección de intrusos (IDS), lo que impide identificar actividades maliciosas de forma oportuna.

A partir de los resultados obtenidos, se proponen la Implementación de un IDS (Suricata) como sistema de detección de intrusos basado en red (NIDS), aprovechando su capacidad de inspección profunda de paquetes (DPI), su naturaleza de código abierto y su compatibilidad con reglas Snort y colocar políticas de control de acceso, cierre de puertos innecesarios y segmentación de red para limitar la exposición a ataques.

Implementar un sistema de autenticación personalizada (no compartida) y rotación periódica de contraseñas, junto con autenticación de dos factores cuando sea posible.

La presente investigación demuestra que las instituciones de nivel medio superior presentan vulnerabilidades críticas en sus redes (accesos sin control, puertos abiertos, contraseñas compartidas), lo que las convierte en blancos potenciales de ciberataques. La implementación de un IDS como Suricata, combinado con el blindaje de redes, no solo permite detectar actividades maliciosas en tiempo real, sino que también fortalece la gobernanza tecnológica y la protección de datos sensibles (calificaciones, información personal, registros administrativos).

Sin embargo, se reconoce que la tecnología por sí sola no resuelve el problema. Factores humanos (falta de capacitación, malas prácticas), organizacionales (ausencia de políticas claras) y técnicos (falsos positivos, recursos limitados) deben ser atendidos de manera integral. El enfoque sistémico y pragmático adoptado permitió diseñar soluciones viables, pero su efectividad dependerá de su correcta operación y mantenimiento.

Figura 7

Fases de implementación de IDS

Nota: Desarrollo del autor

CONCLUSIONES

En conclusión, la investigación logró identificar las vulnerabilidades específicas de las redes escolares de nivel medio superior y demostró que la implementación conjunta de Suricata y el blindaje de redes es una solución técnica viable, de bajo costo y efectiva para detectar intrusiones, reducir incidentes y proteger la información institucional. No obstante, su éxito a largo plazo requiere capacitación continua, actualización constante de reglas y políticas claras de privacidad. Este estudio responde afirmativamente a la pregunta de factibilidad y proporciona un modelo replicable para otras instituciones educativas con recursos limitados.

REFERENCIAS BIBLIOGRÁFICAS

Babbie, E. (2020). The Practice of Social Research (15th ed.). Cengage Learning.

Campbell, D. T., & Stanley, J. C. (1963). Experimental and Quasi-Experimental Designs for Research. Houghton Mifflin Company.

Cilleruelo, C. (2022, September 8). ¿Qué es Suricata en ciberseguridad? KeepCoding Bootcamps. https://keepcoding.io/blog/que-es-suricata-en-ciberseguridad/

Cloudflare. (2022). Using Suricata for network threat detection at scale. Cloudflare Security Blog. Recuperado de https://blog.cloudflare.com/suricata-threat-detection-at-scale/

Cómo detectar malware con reglas de Suricata. (n.d.). CEC. Retrieved September 26, 2024, from https://www.cec.es/como-detectar-malware-con-reglas-de-suricata/

Cruzito. (2020, noviembre 3). Stanley Miller: teoría, experimento y aparato. Estudyando. https://estudyando.com/stanley-miller-teoria-experimento-y-aparato/

De vulnerabilidad a fortaleza: Implementación exitosa de Suricata IDS. (2024, January 18). Guías Open Source. https://guiasopensource.net/seguridad-en-codigo-abierto/vulnerabilidad-fortaleza-implementacion-exitosa-suricata-ids

García, L. (2021). Implementación de un Sistema de Detección de Intrusos basado en Suricata en la red académica de la UANL [Tesis de maestría no publicada]. Universidad Autónoma de Nuevo León.

Gobierno de Cantabria. (2021). Protección de infraestructura crítica con Suricata y Wazuh. Dirección General de Innovación y Digitalización.

Parra, A. (2020, enero 16). Tipos de estudio de investigación y sus características. QuestionPro. https://www.questionpro.com/blog/es/tipos-de-investigacion-2/

¿Qué es metodología de la investigación según Mario Bunge? (2023, junio 23). Tus-consejos.com. https://tus-consejos.com/que-es-metodologia-de-la-investigacion-segun-mario-bunge/

Rodríguez, M. (2020). Análisis comparativo entre Snort y Suricata en la red de posgrado de la UDG. Revista Iberoamericana de Seguridad Informática, *12*(2), 45–60.

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research Methods for Business Students (8th ed.). Pearson.

Suricata - IDS/IPS - Instalación, configuración básica reglas. (n.d.). Blog Elhacker.net. Retrieved September 26, 2024, from https://blog.elhacker.net/2021/03/suricata-ids-ips-instalacion-configuracion-reglas-.html

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). SAGE Publications.

